("Arnold"), claims 3 and 4 under 35 U.S.C. § 103(a) as being unpatentable over Arnold in view of Applicant Admitted Prior Art ("AAPA") and further in view of U.S. Patent No. 6,714,649 to Masuda et al ("Masuda"), and claims 5-20 under 35 U.S.C. § 103(a) as being unpatentable over Arnold in view of AAPA and Masuda and further in view of U.S. Patent No. 5,933,501 to Leppek ("Leppek"). Applicants respectfully traverse the foregoing bases for rejection.

Applicants' present invention is directed to a method for securely providing encryption keys for encrypting and decrypting data. According to the present invention, an encryption key is generated and used to encrypt data. The encryption key is split into two components by generating a first key portion and then calculating the second key portion using the first key portion and the key, such that the combination of the first key portion and the second key portion yield the key. The first and second key portions can be provided separately to the recipient of the data in order to maintain the secrecy of the key. The first and second key portions are combined to yield the key, which is used to decrypt the data. As such, the same key is used both to encrypt and decrypt the data. These limitations are articulated in claim 1 (and, therefore, in each of its dependent claims 2-10), which recites:

> generating a first encryption key;
>
> encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product;
>
> generating a first key portion of said first encryption key;
>
> calculating a second key portion by utilizing said first key portion and said first encryption key to generate a said second key portion such that the combination of said first key portion and second key portion form said first encryption key;
>
> providing said first key portion and said second key portion and said encrypted initial software product for use in a hardware product;
>
> combining said first key portion and said second key portion to provide said first encryption key in said hardware product; and

> utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product.

The examiner has stated that Arnold discloses these limitations at col. 6, l. 66 through col. 7, l. 44, and in FIG. 3 (ref. nos. 130-180). Applicants respectfully disagree and submit that Arnold does not teach or suggest Applicants' claimed invention. Instead, Arnold teaches distribution of data using a public key encryption system using, for example, the RSA algorithm. More particularly, Arnold teaches encryption of data using a sender's private key, and decryption of the data using a receiver's public key. A digital signature can accompany the transmitted data. In one embodiment, Arnold teaches the use of a symmetric key to both encrypt and decrypt the data. However, in this embodiment, the symmetric key itself is encrypted and decrypted using public key encryption. Importantly, Arnold does not in either embodiment teach or suggest splitting an encryption key into two components that can be combined to yield the encryption key, and Arnold particularly does not in either embodiment teach or suggest splitting an encryption key into first and second key portions wherein the first key portion is generated and the second key portion is calculated from the encryption key and the first key portion such that the combination of the first key portion and the second key portion form the encryption key. In view of the foregoing, Applicants respectfully submit that the examiner's rejection of claims 1 and 2 under 35 U.S.C. 102 § 102(e) as anticipated by Arnold is not supported and that the examiner's rejections of dependent claims 3-10 under 35 U.S.C. § 103(a) based on Arnold in combination with other cited references are moot. Accordingly, Applicants respectfully request that the examiner withdraw the rejections of these claims.

Independent claim 11 (and, therefore, each of its dependent claims 12-20) recites limitations similar to those discussed above in connection with claim 1, namely:

> providing a first encryption key;
>
> encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product;
>
> providing a first key portion;
>
> utilizing said first key portion and said first encryption key to calculate a second key portion such that the combination of said first and second key portions form said first encryption key;
>
> * * *
>
> combining said first key portion and said second key portion to provide said first encryption key in said hardware product; and
>
> utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product.

As discussed above in connection with claim 1, Applicants respectfully submit that Arnold does not teach or suggest the limitations directed to encrypting the initial software product with a first encryption key to generate an encrypted initial software product; providing a first key portion; utilizing the first key portion and the encryption key to calculate a second key portion such that the combination of the first and second key portions form the encryption key; combining the first key portion and the second key portion to provide the first encryption key; and using the encryption key to decrypt the data. As such, Applicants respectfully submit that Arnold does not provide a basis for the examiner's rejection under 35 U.S.C. § 103(a) of claims 11-20. Accordingly, Applicants respectfully request that the examiner withdraw the rejections of thee claims.

Based on the above, Applicants respectfully submit that the pending claims are allowable over the cited prior art and respectfully requests reconsideration toward that end.

Respectfully submitted,

Date: November 8, 2004

Mark P. Vrla
Registration No. 43,973
Attorney for Applicant

JENNER & BLOCK LLP
One IBM Plaza
Chicago, IL 60611
Ph. (312) 222-9350
Fax (312) 840-7657